BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-003455
(43)Date of publication of application : 06.01.1999

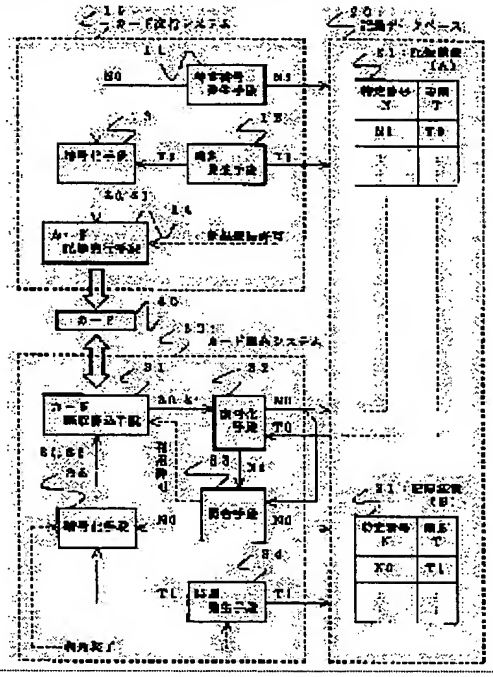
(51)Int.Cl. G07D 9/00
G07D 9/00
G06F 17/60
G06F 19/00
G06K 17/00
G07F 7/08
G07G 1/12

(21)Application number : 09-156400
(22)Date of filing : 13.06.1997

(71)Applicant : NEC CORP
(72)Inventor : SATO YASUSHI

(54) ISSUING AND COLLATING METHOD FOR ELECTRONIC MONEY CARD AND ITS SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To make it difficult to forge or alter a card through recording medium.
SOLUTION: This method generates time data T0 that is a random number and a specific number N0 of a card 40 when a card is issued and records them on a recorder 21 outside the card 40, wherein the number N0 is a cipher data C1 with the data T0 as a key, and the data S1 and the number N0 are recorded on the card 40 and issued. At the time of using a card, the data T0 is retrieved from the recorder 21 based on the number N0 which is read from the card 40, the ciphered data is decoded by decoding the data S1 which is separately read from the card 40 with the data T0 as a key and the card is allowed to be used through collation coincidence. When the card 40 is returned, a cipher data S2 which is enciphered by a time data T1 that newly occurs is generated and recorded on the card 40 and the recorder 21. When an enciphered data is a card utilization number, alteration becomes even more difficult.



LEGAL STATUS

[Date of request for examination] 13.06.1997
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number] 2943861
[Date of registration] 25.06.1999
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

(19)日本国特許庁(JP)　(12)**公開特許公報（A）**　(11)特許出願公開番号

特開平１１－３４５５

(43)公開日　平成11年(1999)1月6日

(51)Int.Cl.[6]		識別記号	FI		
Ｇ０７Ｄ	9/00	４６１	Ｇ０７Ｄ	9/00	４６１　Ｂ
		４３６			４３６　Ｚ
Ｇ０６Ｆ	17/60		Ｇ０６Ｋ	17/00	Ｌ
	19/00		Ｇ０７Ｇ	1/12	３２１　Ｐ
Ｇ０６Ｋ	17/00		Ｇ０６Ｆ	15/21	３４０　Ａ

審査請求　有　請求項の数１９　ＯＬ　（全１８頁）最終頁に続く

(21)出願番号　特願平9-156400

(22)出願日　平成9年(1997)6月13日

(71)出願人　000004237
日本電気株式会社
東京都港区芝五丁目7番1号

(72)発明者　佐藤　靖士
東京都港区芝五丁目7番1号　日本電気株式会社内

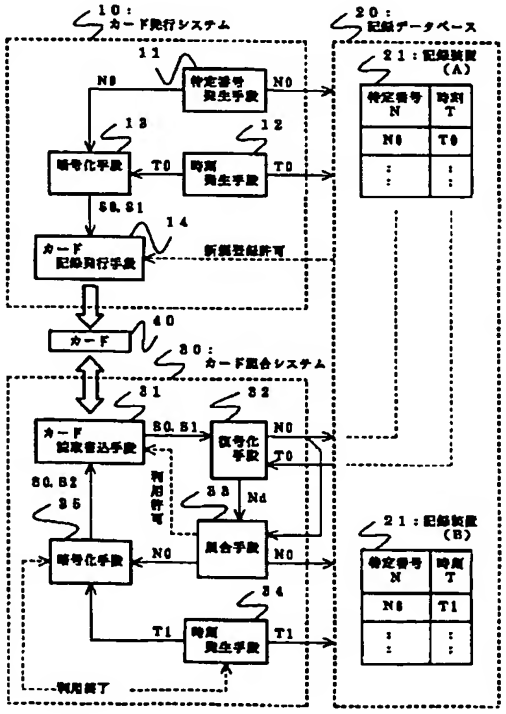
(74)代理人　弁理士　後藤　洋介　（外2名）

(54)【発明の名称】電子貨幣カードの発行照合方法およびその方式

(57)【要約】

【課題】　記録媒体によるカードの偽造または改ざんを困難にすること。

【解決手段】　カード発行の際には、乱数である時刻データＴ0 とカード４０の特定番号Ｎ0 とを生成してカード４０外の記録装置２１に記録し、時刻データＴ0 を鍵として特定番号Ｎ0 を暗号化データＳ1 とし、暗号化データＳ1 と特定番号Ｎ0 とをカード４０に記録して発行する。カード利用の際には、カード４０から読み取った特定番号Ｎ0 に基づき記録装置２１から時刻データＴ0 を検索し、時刻データＴ0 を鍵として別にカード４０から読取った暗号化データＳ1 を復号して暗号化されたデータを復号し、照合一致でカード利用を許可している。カード４０の返却に際しては、改めて発生した時刻データＴ1 により暗号化された暗号化データＳ2 が生成され、カード４０および記録装置２１に記録される。暗号化されるデータがカード使用回数の場合、更に改ざんが困難である。



1

【特許請求の範囲】

【請求項１】　記録媒体であるカードを発行し、このカードにより支払いの精算をする際、カードの照合を行う電子貨幣カードの発行照合方法式において、カード発行システムと記録データベースとカード照合システムとを備え、前記カードは書込み読取り可能な記録媒体であり、前記記録データベースは各種データを記録する一方、検索を受けて送出し、前記カードを発行する際に、前記カード発行システムは、発行する前記カードを一意に特定する特定番号を発生すると共にランダムな数字の発行時乱数を発生し、次いで一方では前記発行時乱数を鍵データとして発生した前記特定番号および別に設定した特定数字の少くとも一方を暗号化した発行時暗号化データを作成し暗号化データにするこの前記発行時暗号化データと前記特定番号とを前記カードに記録して発行し、他方では発生した前記特定番号に対応して前記発行時乱数を乱数として前記記録データベースへ送って記録し、かつ前記カードを利用の際、前記カード照合システムは、カードから記録された特定番号および暗号化データを読み出し、この特定番号に基づいて前記記録データベースから前記特定番号に対応する乱数を索引し、前記カードから読み出された暗号化データをこの索引された乱数により復号し、得られた照合用復号符号を前記特定番号と照合して一致した場合に前記カードの利用を許可することを特徴とする電子貨幣カードの発行照合方法。

【請求項２】　請求項１において、前記カード照合システムが、ランダムな数字の照合時乱数を発生し、前記カードの利用許可があった際に前記特定番号を前記照合時乱数により暗号化した照合時暗号化データを作成し、一方ではこの照合時暗号化データを前記カードに記録されている暗号化データに上書き記録し、他方では発生した前記照合時乱数を前記記録データベースへ送って記録されている乱数に上書き記録することを特徴とする電子貨幣カードの発行照合方法。

【請求項３】　請求項１において、前記カードに記録する際、前記特定番号は特定の暗号化鍵により暗号化し、カード照合の際、この特定の暗号化鍵により復号して用いることを特徴とする電子貨幣カードの発行照合方法。

【請求項４】　記録媒体であるカードを発行し、このカードにより支払いの精算をする際、カードの照合を行う電子貨幣カードの発行照合方法において、カード発行システムと記録データベースとカード照合システムとを備え、前記カードは書込み読取り可能な記録媒体であり、前記記録データベースは各種データを記録する一方、検索を受けて送出し、前記カードを発行する際には、前記カード発行システムは、発行する前記カードを一意に特定する特定番号を発生すると共にランダムな数字の発行時乱数を発生し、これら特定番号および発行時乱数を前記記録データベースへ送り、次いで記録データベースは、一方では受けた特定番号とこの特定番号に対応する

2

乱数として前記発行時乱数を記録格納すると共に、他方では受けた特定番号を発行時乱数を暗号化鍵として暗号化した発行時暗号化データを作成して前記カード発行システムへ送り、次いで、カード発行システムは、受けた前記発行時暗号化データを暗号化データとして前記特定番号と共に前記カードに記録して発行し、かつ前記カードを利用の際には、前記カード照合システムは、カードから記録された特定番号および暗号化データを読み出して前記記録データベースへ送り、次いでこの記録データベースは、この特定番号に基づいて前記記録データベースから前記特定番号に対する乱数を索引し、これら特定番号および乱数に基づいて特定番号を乱数により暗号化した照合用暗号化データを作成しこの照合用暗号化データをカードから読み出した前記暗号符号と照合して一致したことを前記カード照合システムへ送り、次いでカード照合システムが照合一致を受けた場合に前記カードの利用を許可することを特徴とする電子貨幣カードの発行照合方法。

【請求項５】　請求項４において、前記カード照合システムが、ランダムな数字の照合時乱数を発生して前記記録データベースへ送り、前記カードの利用許可があった際に、前記記録データベースが、前記特定番号を前記照合時乱数により暗号化した照合時暗号化データを作成し、一方では記録されている乱数を照合時乱数に上書き記録し、他方では前記カード照合システムへ送り前記照合時暗号化データを前記カードに記録されている暗号化データに上書き記録することを特徴とする電子貨幣カードの発行照合方法。

【請求項６】　請求項１、２、３、４、または請求項５において、前記特定番号は、カードを発行する複数の前記発行装置それぞれで発生する通し番号と、前記カードを一意に特定できるように前記発行装置それぞれに予め付与された装置識別子とにより構成されていることを特徴とする電子貨幣カードの発行照合方法。

【請求項７】　請求項１、２、３、４、または請求項５において、前記乱数はその時点の時刻を参照した時刻データであることを特徴とする電子貨幣カードの発行照合方法。

【請求項８】　請求項１、２、３、４、または請求項５において、前記特定番号は請求項６に記載の通し番号および装置識別子により構成され、かつ前記乱数はその時点の時刻を参照した時刻データであることを特徴とする電子貨幣カードの発行照合方法。

【請求項９】　請求項１、２、３、４、５、６、７、または請求項８において、前記カード発行システムは、更に、利用実績の初期値を発生し、この利用実績の初期値データを前記カードに記録して発行すると共に前記記録データベースに記録し、かつ前記カード照合システムは、更に、利用毎に利用実績データを更新する一方、カード照合の都度、前記カードに記録されている利用実績

データを更新すると共に前記記録データベースの記録を更新することを特徴とする電子貨幣カードの発行照合方法。

【請求項１０】　請求項９において、前記特定番号に代り前記利用実績データが前記乱数により暗号化されることを特徴とする電子貨幣カードの発行照合方法。

【請求項１１】　記録媒体であるカードを発行し、このカードにより支払いの精算をする際、カードの照合を行う電子貨幣カードの発行照合方式において、カード発行システムと記録データベースとカード照合システムとを設け、前記カードは、書込み読取り可能な記録媒体であり、前記カード発行システムは、発行する前記カードを一意に特定する特定番号をカードを発行する際に発生して出力する特定番号発生装置と、ランダムな数字の発行時乱数を発生して出力する発行時乱数発生装置と、カードを発行する際に発生した前記特定番号および前記発行時暗号化データを受け、前記発行時乱数を暗号化鍵として前記特定番号を暗号化した発行時暗号化データを作成しこの発行時暗号化データを出力する暗号化装置と、この暗号化装置から出力された発行時暗号化データを暗号化データとして前記特定番号と共に前記カードに記録して発行するカード記録発行装置と、カードを発行する際に発生した前記特定番号および前記発行時暗号化データを受けて前記記録データベースへ転送する第１のデータ通信装置とを備え、前記記録データベースは、前記特定番号と共に、乱数として前記発行時乱数を記録する記録装置と、指示を受けてこの記録装置のデータを検索し検索結果を出力するデータ検索装置と、このデータ検索装置を介して前記記録装置へ前記第１のデータ通信装置から受ける特定番号および発行時暗号化データを転送し、前記カード照合システムから受ける特定番号を前記データ検索装置に転送し検索された前記乱数を前記カード照合システムへ返送する第２のデータ通信装置とを備え、かつ、前記カード照合システムは、前記カードを利用の際にカードに記録された特定番号および暗号化データを読み出して送出する一方、カードの利用許可により所定のカード精算処理を終了した際にカードに所定データを記録するカード読取書込装置と、このカード読取書込装置から受けた特定番号を前記記録データベースへ送出し結果として受けた乱数を復号化鍵として前記特定番号を復号した復号符号を生成し出力する復号化装置と、この生成された復号符号を前記特定番号と照合して一致した際に利用許可を前記カード読取書込装置へ送る照合装置と、受けた特定番号を前記記録データベースへ転送しこの結果として受ける乱数を前記復号化装置へ送る第３のデータ通信装置とを備えることを特徴とする電子貨幣カードの発行照合方式。

【請求項１２】　請求項１１において、前記カード照合システムがランダムな数字の照合時乱数を発生する照合時乱数発生装置を更に備え、前記暗号化装置は前記カードの利用許可があった際に前記照合時乱数を暗号化鍵として前記特定番号を暗号化した照合時暗号化データを作成して出力し、前記カード読取書込装置はこの照合時暗号化データを前記カードに記録されている暗号化データに上書き記録し、第３のデータ通信装置は発生した前記照合時乱数を前記記録データベースへ送出し、前記記録データベースは記録されている乱数に受けた前記照合時乱数を上書き記録することを特徴とする電子貨幣カードの発行照合方式。

【請求項１３】　記録媒体であるカードを発行し、このカードにより支払いの精算をする際、カードの照合を行う電子貨幣カードの発行照合方式において、カード発行システムと記録データベースとカード照合システムとを設け、前記カードは、書込み読取り可能な記録媒体であり、前記カード発行システムは、発行する前記カードを一意に特定する特定番号を前記カードを発行する際に発生し出力する特定番号発生装置と、ランダムな数字の発行時乱数を発生し出力する発行時乱数発生装置と、発行時乱数を暗号化鍵として前記特定番号を暗号化した発行時暗号化データを暗号化データとして前記特定番号と共に前記カードに記録して発行するカード記録発行装置と、前記特定番号および発行時乱数を前記記録データベースへ送りこの結果記録データベースから受ける前記発行時暗号化データを前記カード記録発行装置へ転送する第１のデータ通信装置とを備え、前記記録データベースは、受けた前記特定番号およびこの特定番号に対応する前記乱数を記録する記録装置と、前記カード発行システムおよび前記カード照合システムそれぞれとデータを授受する第２のデータ通信装置と、この第２のデータ通信装置を介して受ける前記特定番号に基づいて前記記録装置から対応する乱数を検索し出力するデータ検索装置と、一方では前記第２のデータ通信装置を介してカード発行システムから特定番号および発行時乱数を受け発行時乱数を暗号化鍵としてこの特定番号を暗号化した発行時暗号化データを作成して前記カード発行システムへ返送し、他方では前記第２のデータ通信装置を介して前記カード照合システムから受けた特定番号をこの特定番号に基づいて前記データ検索装置を介して検索により得た乱数を暗号化鍵として暗号化した照合用暗号化データを生成し出力する暗号化装置と、この暗号化装置から出力された照合用暗号化データと前記カード照合システムから受ける暗号化データとを照合し一致した場合に前記カードの利用許可を前記第２のデータ通信装置を介してカード照合システムへ送出する照合装置とを備え、かつ前記カード照合システムは、前記記録データベースとデータを授受する第３のデータ通信装置と、前記カードを利用の際に、カードに記録された特定番号および暗号化データを読み出し前記第３のデータ通信装置を介して前記記録データベースへ送り、この記録データベースの前記照合装置から照合一致を受け所定のカード精算処理を終

了した際にカードに所定のデータを記録するカード読取書込装置とを備えることを特徴とする電子貨幣カードの発行照合方式。

【請求項１４】　請求項１３において、前記カード照合システムがランダムな数字の照合時乱数を発生し出力する照合時乱数発生装置を更に備え、この発生した照合時乱数を前記第３のデータ通信装置が前記記録データベースへ転送し、前記記録データベースでは、前記記録装置が前記第２のデータ通信装置を介して受けた照合時乱数により記録されている乱数を上書き記録更新し、暗号化装置が前記カードの利用許可があった際に、前記第２のデータ通信装置を介して受けた前記照合時乱数を暗号化鍵として前記特定番号を暗号化した照合時暗号化データを作成して出力し、この照合時暗号化データを前記第２のデータ通信装置が前記カード照合システムへ転送し、前記カード照合システムでは、前記カード読取書込装置が前記第３のデータ通信装置を介して受けた前記照合時暗号化データを前記カードに記録されている暗号化データに上書き記録することを特徴とする電子貨幣カードの発行照合方式。

【請求項１５】　請求項１１、１２、１３、または請求項１４において、前記特定番号は、カードを発行する複数の前記発行装置それぞれで発生する通し番号と、前記カードを一意に特定できるように前記発行装置それぞれに予め付与された装置識別子とにより構成されていることを特徴とする電子貨幣カードの発行照合方式。

【請求項１６】　請求項１１、１２、１３、または請求項１４において、前記乱数は、その時点の時刻を参照した時刻データであることを特徴とする電子貨幣カードの発行照合方式。

【請求項１７】　請求項１１、１２、１３、または請求項１４において、前記特定番号は、請求項１５に記載の通し番号および装置識別子により構成され、かつ前記乱数は、その時点の時刻を参照した時刻データであることを特徴とする電子貨幣カードの発行照合方式。

【請求項１８】　請求項１１、１２、１３、１４、１５、１６、または請求項１７において、前記カード発行システムは、更に、利用実績の初期値データを発生する利用実績初期値発生装置を備え、この利用実績の初期値データを前記カードに記録して発行すると共に前記記録データベースに記録し、かつ前記カード照合システムは、更に、利用毎に利用実績データを更新する利用実績更新装置を備え、カード照合の都度、カードに記録されている利用実績データを更新すると共に前記記録データベースの記録を更新することを特徴とする電子貨幣カードの発行照合方式。

【請求項１９】　請求項１８において、前記特定番号の代りに、前記利用実績データが前記乱数を暗号化鍵として暗号化されることを特徴とする電子貨幣カードの発行照合方式。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、記録媒体であるカードを発行し、このカードにより支払いの精算をする際、カードの照合を行う電子貨幣カードの発行照合方式に関し、特に、カードに使用する記録媒体を単純化し、かつカードの偽造または不正使用を防止出来る電子貨幣カードの発行照合方式に関する。

【０００２】

【従来の技術】従来、この種の電子貨幣カードの発行照合方式では、カードの認証に際して、カードの偽造または改ざんを防止するために、表面に顔写真を貼付けもしくは印刷したＩＤ（個人識別）カード、ＩＣ（集積回路）による演算機能を内蔵するカードなどが用いられる。

【０００３】表面の顔写真に対する技術が、例えば、特開平８－３０５８１６号公報に記載されている。

【０００４】この構成では、カード上の顔写真の特徴的な画像情報を、スクランブル圧縮による少い情報量でカードに記録することにより、照合装置で、顔写真の画像情報を高速で読み出し、カード上の顔写真が偽造・改ざんされていないかを迅速に判定している。

【０００５】一方、ＩＣ内蔵のカードについての技術が、例えば、特開平８－２８７２０２号公報に記載されている。

【０００６】この方式では、ＩＣカードとサービス提供側のセンタとの両者に内蔵される暗号化関数が認証を偽造するものに盗まれてもカードの認証に対する安全性を高くするため、暗号化鍵と、センタから受けた乱数とを、暗号化関数に基づいてカード側が演算し、この演算結果をカードからセンタへ送り、カード側の演算結果とセンタで同様に演算した演算結果とをセンタで照合する場合に、センタ側からカードへ送る乱数のビット長をランダムに制御できるようにしたものである。

【０００７】

【発明が解決しようとする課題】上述した従来の電子貨幣カードの発行照合方式のうち、上記公開公報に記載された顔写真の画像情報による方式では、カード上の画像情報とこの画像情報の圧縮データとが照合されるため、画像データの圧縮方式が盗まれた場合には、盗まれた圧縮方式を用いて改ざんされた顔写真の画像情報から得た圧縮データがカードに記録できるので、安全性に疑問があるという問題点がある。

【０００８】すなわち、同一カード上のデータの整合性によってカードの認証を行う方式では、データの変換手段である暗号化手段が判明した場合にカードの偽造は比較的容易である。

【０００９】また、上記公開公報に記載されたＩＣカードによる方式では、カード内に複雑な機能をもたせるため、改ざんは困難になるが、カードそのもののコストが

かかり、例えば、プリペイドカードのように多量に使用してもらうには実用上の面で不向きであるという問題点がある。

【００１０】本発明の課題は、上記問題点を解決して、カードに使用する記録媒体を単純化し、かつカードの偽造または不正使用を防止できる電子貨幣カードの発行照合方式を提供することである。

【００１１】

【課題を解決するための手段】本発明による第１の電子貨幣カードの発行照合方法は、記録媒体であるカードを発行し、このカードにより支払いの精算をする際、カードの照合を行う電子貨幣カードの発行照合方法において、カード発行システムと記録データベースとカード照合システムとを備え、前記カードは書込み読取り可能な記録媒体であり、前記カードを発行する際に、前記カード発行システムは、発行する前記カードを一意に特定する特定番号を発生すると共に、ランダムな数字の発行時乱数を発生し、次いで一方では前記発行時乱数を鍵データとして発生した前記特定番号および別に設定した特定数字の少くとも一方を暗号化した発行時暗号化データを作成し、暗号化データにするこの前記発行時暗号化データと前記特定番号とを前記カードに記録して発行し、他方では発生した前記特定番号に対応して前記発行時乱数を乱数として前記記録データベースへ送って記録し、かつ前記カードを利用の際、前記カード照合システムは、カードから記録された特定番号および暗号化データを読み出し、この特定番号に基づいて前記記録データベースから前記特定番号に対応する乱数を索引し、前記カードから読み出された暗号化データをこの索引された乱数により復号し、得られた照合用復号符号を前記特定番号と照合して一致した場合に前記カードの利用を許可している。

【００１２】この方法によれば、カードは、単に書込み読み出し可能な記録媒体でよい。また、各システムでの暗号化方式が固定していても暗号化鍵データが各カードにより異なるうえ、暗号化鍵データを記録保管する記録データベースをカード発行場所またはカード照合場所のいずれからも離すことができるので、カード、カード発行システム、またはカード照合システムのみに在るデータだけでは認証可能なカードに改ざんすることは困難である。

【００１３】また、上記第１の発明に対して前記カード照合システムが、ランダムな数字の照合時乱数を発生し、前記カードの利用許可があった際に前記照合時乱数を暗号化鍵として前記特定番号を暗号化した照合時暗号化データを作成し、一方ではこの照合時暗号化データを前記カードに記録されている暗号化データに上書き記録し、他方では発生した前記照合時乱数を前記記録データベースへ送って記録されている乱数に上書き記録している。

【００１４】この構成により、記録データベースおよびカードの暗号化鍵データがカードを利用する度に変更され、共通の暗号化鍵データを使用していないので、暗号化鍵データが盗まれた場合でも暗号の解読を困難にしており、改ざんによる安全性は更に高くなる。

【００１５】本発明による第２の電子貨幣カードの発行照合方法は、カード発行システムと記録データベースとカード照合システムとを備え、前記カードは、書込み読取り可能な記録媒体であり、前記カードを発行する際には、前記カード発行システムは、発行する前記カードを一意に特定する特定番号を発生すると共にランダムな数字の発行時乱数を発生し、これら特定番号および発行時乱数を前記記録データベースへ送り、次いで記録データベースは、一方では受けた特定番号とこの特定番号に対応する乱数として前記発行時乱数を記録格納すると共に、他方では受けた特定番号を発行時乱数を暗号化鍵として暗号化した発行時暗号化データを作成して前記カード発行システムへ送り、次いで、カード発行システムは、受けた前記発行時暗号化データを暗号化データとして前記特定番号と共に前記カードに記録して発行し、かつ前記カードを利用の際には、前記カード照合システムは、カードから記録された特定番号および暗号化データを読み出して前記記録データベースへ送り、次いでこの記録データベースは、この特定番号に基づいて前記記録データベースから前記特定番号に対する乱数を索引し、これら特定番号および乱数に基づいて特定番号を乱数により暗号化した照合用暗号化データを作成しこの照合用暗号化データをカードから読み出した前記暗号符号と照合して一致したことを前記カード照合システムへ送り、次いでカード照合システムが照合一致を受けた場合に前記カードの利用を許可している。

【００１６】この構成によれば、上記第１の発明から復号化手段を不要にしたにも拘らず、第１の発明同様な作用を有し、かつ暗号化手段が記録データベースに集中されているので、複数のカード照合システムを簡素化できる。

【００１７】また、第２の発明においても、前記カード照合システムが、ランダムな数字の照合時乱数を発生して前記記録データベースへ送り、前記カードの利用許可があった際に、前記記録データベースが、前記照合時乱数を暗号化鍵として前記特定番号を暗号化した照合時暗号化データを作成し、一方では記録されている乱数を照合時乱数に上書き記録し、他方では前記カード照合システムへ送り前記照合時暗号化データを前記カードに記録されている暗号化データに上書き記録することにより、上記第１の発明同様の作用を有している。

【００１８】また、乱数を時刻データとすることにより通常有する時計を利用することができるので、特別な乱数発生装置を不要にできる。また、カードの利用実績データを加味して整合性を調べることにより、カード内容

の改ざんなどによる不正使用を更に簡単に発見することができる。

【００１９】

【発明の実施の形態】次に、本発明の実施の形態について図面を参照して説明する。

【００２０】図１は本発明の実施の一形態を示す機能ブロック図である。図１に示された電子貨幣カードの発行照合方式では、カード媒体をカードとして新規にカードを発行するカード発行システム１０、カードに関する各種データを記録格納する記録データベース２０、およびカード利用の際、利用するカードを記録データベース２０のデータに基づいて照合し、カード利用の可否を決定するカード照合システム３０それぞれが設けられているものとし、カード４０には一般の書込み読取り可能な記録媒体が用いられるものとする。

【００２１】カード発行システム１０は特定番号発生手段１１、時刻発生手段１２、暗号化手段１３、およびカード記録発行手段１４を備えるものとする。記録データベース２０は記録装置２１を備えるものとする。また、カード照合システム３０は、カード読取書込手段３１、復号化手段３２、照合手段３３、時刻発生手段３４、および暗号化手段３５を備えるものとする。

【００２２】カード発行システム１０の特定番号発生手段１１は、本カード発行照合システム内で多数のカードそれぞれに対して一意の番号を特定番号N0 としてカード発行の際に発生するものとする。時刻発生手段１２は、カード発行の時刻を認識できると共に、２４時間にわたって異なる数字を順次発生するので乱数発生手段として用いられ、カード発行の際に発生している時刻データT0 を暗号化手段１３における暗号化鍵にするものとする。

【００２３】また、暗号化手段１３は、固定された特定暗号化鍵と、時刻発生手段１２が発生した時刻データT0 による暗号化鍵とにより、特定番号発生手段１１が発生した特定番号N0 を暗号化した暗号化データS0 ，S1 それぞれを生成し、この暗号化データS0 ，S1 をカード記録発行手段１４へ送るものとする。

【００２４】カード記録発行手段１４は、記録データベース２０から新規登録許可を受けた際、暗号化手段１３から受ける暗号化データS0 ，S1 をカード４０の記録領域に記録した後、排出により発行するものとする。

【００２５】記録データベース２０の記録装置２１は、特定番号Nとこの特定番号Nに対して適用される時刻データTとを記録する記憶領域を有し、まず、カード発行システム１０で特定番号発生手段１１が発生した特定番号N0 と時刻発生手段１２が発生した時刻データT0 とを記録装置２１（A）として記録するものとする。また、カード照合システム３０でカード４０の照合の際には、時刻発生手段３４が発生した時刻データT1 により記録装置２１（B）に示されるように上書きされるものとする。

【００２６】カード照合システム３０のカード読取書込手段３１は、利用するカード４０をセットされた際に、カード４０に記録されている暗号化データS0 ，S1 それぞれを読取り、復号化手段３２へ送る。一方、カード読取書込手段３１は照合手段３３から利用許可を受けた際には暗号化手段３５から受ける暗号化データS0 ，S2 をカード４０に上書き記録してカード４０を排出することによりカード利用者に返却するものとする。

【００２７】復号化手段３２は、一方では特定暗号化鍵により暗号化データS0 を復号して特定番号N0 を生成し、生成された特定番号N0 に基づいて記憶データベース２０の記録装置２１（A）から時刻データT0 を検索して読取り受取る。復号化手段３２は、他方では記録装置２１から受ける時刻データT0 を復号化鍵とし、カード読取書込手段３１から受けた暗号化データS1 を復号して復号符号Nd を生成し、照合手段３３へ送る。復号符号Nd は、正常に認証できるカード４０であれば特定番号N0 である。

【００２８】照合手段３３は、一方では復号化手段３２から復号符号Nd を受け、他方では復号化手段３２で暗号化データS0 から復号された特定番号N0 を受けて両者を照合し、一致した特定番号N0 を記録データベース２０および暗号化手段３５それぞれへ出力するものとする。また、照合一致は利用許可としてカード読取書込手段３１へ通知されるものとする。

【００２９】時刻発生手段３４は、カード照合時刻を認識すると共に、乱数発生手段でもあり、２４時間にわたり暗号化鍵となる数字を順次発生する。従って、時刻発生手段３４は、カード照合の際に発生する時刻データT1 を、暗号化鍵にすると共に記録装置２１へ送るものとする。

【００３０】暗号化手段３５は、一方では照合手段３３から照合一致した特定番号N0 を受け、他方では時刻発生手段３４が発生する時刻データT1 を受け、カード発行システム１０と同様、一方では固定された特定暗号化鍵により特定番号N0 を暗号化した暗号化データS0 、他方では時刻発生手段３２が発生した時刻データT1を暗号化鍵として特定番号N0 を暗号化した暗号化データS2 、それぞれを生成し、カード記録発行手段１４へ送るものとする。

【００３１】時刻発生手段３４から記録装置２１へ送られた時刻データT1 は記録装置２１（A）における時刻データT0 に上書きされることにより、記録装置２１（B）に図示されるように時刻データTが更新される。

【００３２】次に、図１に図２を併せ参照して、カード発行手順（A）およびカード照合手順（B）について説明する。

【００３３】カード発行システム１０において、カード発行要求が発生した際、まず特定番号発生手段１１が特

定番号N0 を発生し、かつ時刻発生手段１２が時刻データT0 を発生し（手順１０１）、発生した特定番号N0 および時刻データT0 を暗号化手段１３および記録装置２１それぞれへ送る。

【００３４】暗号化手段１３は、特定番号N0 を、特定暗号化鍵により暗号化して暗号化データS0 を作成する一方、時刻データT0 を暗号化鍵として暗号化し暗号化データS1 を作成し（手順１０２）、暗号化データS0 , S1 をカード記録発行手段１４へ送る。一方、記録装置２１では特定番号N0 に対応する時刻データTの領域に時刻データT0 を新規登録する（手順１０３）。

【００３５】手順１０３で新規登録の際、特定番号N0 で記録装置２１に既に時刻データT- が登録済みのように新規登録不可能な場合（手順１０４のNO）、手順は手順１０１から再度、開始される。

【００３６】手順１０４が“ＹＥＳ”で新規登録された場合、カード記録発行手段が、記録データベース２０から新規登録許可を受け、暗号化手段１３から受けた暗号化データS0 , S1 を新規カードに記録し排出することにより、カード４０が発行され（手順105）、カード発行手順は終了する。

【００３７】次に、カード照合システム３０において、カード読取書込手段３１にカード４０を挿入して利用する際、カード読取書込手段３１は挿入されたカード４０から暗号化データS0 , S1 を読取り（手順１１１）、復号化手段３２に送る。

【００３８】復号化手段３２では、受けた暗号化データS0 から特定暗号化鍵により特定番号N0 を再生し、この特定番号N0 を記録データベース２０へ送り、記録装置２１の特定番号N0 領域から時刻データT0 を索引する（手順１１２）。

【００３９】次いで、復号化手段３２は、カード読取書込手段３１から受けた暗号化データS1 を記録装置２１から索引した時刻データT0 を暗号鍵鍵にして復号することにより特定番号Nd を再生して（手順１１３）、照合手段３３へ送る。

【００４０】照合手段３３は復号化手段３２から受けた暗号化データS0 から再生したした特定番号N0 と暗号化データS1 から復号した特定番号Nd とを照合する（手順１１４）。次いで照合手段３３は、照合一致の場合（手順１１５のＹＥＳ）、挿入されたカード４０の利用許可をカード読取書込手段３１へ送る（手順１１６）と共に、一致した特定番号N0 を暗号化手段３５へ送る。

【００４１】この利用許可にしたがってカード４０が利用され、例えば、精算により利用が終了した際、一方では、暗号化手段３５が、時刻発生手段３４で発生する新しい時刻データT1 を受け、この時刻データT1 を暗号化鍵にして既に照合手段３３から受けている特定番号N0 を暗号化し、新しい暗号化データS2 を作成し（手順１１７）、特定番号N0 を特定暗号化鍵により暗号化した暗号化データS0 と共にカード読取書込手段３１へ送る。

【００４２】また、カードの利用が終了した際、他方では、時刻発生手段３４が発生する新しい時刻データT1 と照合手段３３が発生する特定番号N0 とを記録データベース２０が受け、記録装置２１の特定番号N0 領域で時刻データT1 を上書きして更新登録する（手順１１８）。

【００４３】また、暗号化データS0 , S2 とを受けたカード読取書込手段３１は、暗号化データS1 に暗号化データS2 を上書きして更新記録したカード４０を排出することにより（手順１１９）、カード４０をカード利用者に返却する。

【００４４】上記手順１１５が“NO”で照合が不一致の場合、照合手段３３は、カード読取書込手段３１へ挿入されたカード４０が不良として利用不許可を通知する（手順１１６）。

【００４５】上記説明では、単に特定番号発生手段としたが、具体的には、システム全体でカードそれぞれに一意の番号を付与できるように、複数のカード発行システムがある場合、カード発行システムそれぞれに装置番号を識別できる識別子を設定して、この識別子と、これらカード発行システムそれぞれで発生する通し番号とを組合わせて特定番号とすることが、適切な手段として採用できる。また、上記時刻発生手段は、時刻を特定するために用いられる場合、変化する暗号化鍵として適切であるが、変化する暗号化鍵として用いるのみであれば、別の乱数発生装置により発生された乱数を利用してもよい。

【００４６】上記説明では、特定番号を固定の暗号化鍵により暗号化データに変換してカードに記録したが、カード照合システムで復号化手段がない場合には暗号化できないこともあり、カードの特定番号は、そのまま、暗号化なしで記録することでもよい。

【００４７】また、上記説明では毎度可変の時刻または乱数を暗号化鍵として特定番号を暗号化して、本発明の主目的である改ざんの困難さを得ているが、更に利用の都度変更のあるデータ、例えば利用実績を数値化した利用回数データを、特定番号の代わりに暗号化することにより、暗号化データをより複雑にすることができるので、改ざんをより困難にすることもできる。

【００４８】すなわち、カードに付与される特定番号以外の各種データを、それぞれが異なる乱数を持つ暗号化鍵データによって暗号化され、この暗号化された暗号化データをカードに記録し、暗号化される各種データを記録データベースの特定番号領域それぞれに記録することにより、より一層、カードの偽造・改ざんを困難にする。

【００４９】また、上記説明ではカードを挿入し排出す

るとしたが、カードの記録媒体上で書込み・読取りするためにカードを固定する構造は自由であり、上記説明が本発明を限定するものではない。

【００５０】

【実施例】

［第１の実施例］次に、上記図１の形態に基づく第１の実施例について図３および図４を参照して具体的に説明する。図示されるように、電子貨幣カードの発行照合システムは複数のカード発行システム１１０、一つの記録データベース１２０、および複数のカード照合システム１３０により構成され、遠隔地間でデータ通信網を介して相互接続しており、書込み可能な記録媒体によるカード１４０が使用されているものとする。

【００５１】まず、図３を参照して第１の実施例のカード発行システム１１０について説明する。

【００５２】カード１４０を発行するカード発行システム１１０は、特定番号発生装置１１１、時刻発生装置１１２、利用実績初期値発生装置１１３、暗号化装置１１４、カード記録発行装置１１５、およびデータ通信装置１１６を備えているものとする。記録データベース１２０は、記録装置１２１、データ検索装置１２２、およびデータ通信装置１２３を備えているものとする。

【００５３】特定番号発生装置１１１は、カード発行の際に発行されるカード１４０に対して通し番号N- を順次発生し、カード１４０にシステム内で一意のカード番号を付与するため、発行装置識別子M0 を出力するものとする。通し番号N- および発行装置識別子M0 それぞれはカード発行の際に、暗号化装置１１４およびデータ通信装置１１６それぞれへ送られる。

【００５４】時刻発生装置１１２は、現在時刻T0 を時刻データT0 として発生し、カード発行の際に暗号化装置１１４およびデータ通信装置１１６それぞれへ送るものとする。利用実績初期値発生装置１１３は、カード１４０が未使用で利用実績がないことを示す初期値データV0 を発生して、カード発行の際に暗号化装置１１４およびデータ通信装置１１６それぞれへ送る。

【００５５】暗号化装置１１４は、発生した通し番号N0 および発行装置識別子M0 による特定番号と時刻データT0 と、更に利用実績初期値データV0 とを受ける。

【００５６】暗号化装置１１４は、システム固定の暗号化鍵を有し、特定番号発生装置１１１から受ける通し番号N0 および発行装置識別子M0 をこの固有暗号化鍵により暗号化して暗号化データS0 とする一方、時刻発生装置１１２から受ける現在の時刻データT0 を暗号化鍵とし利用実績初期値発生装置１１３から受ける利用実績初期値データV0 を暗号化して暗号化データS1 とし、これら暗号化された二つの暗号化データS0 , S1 をカード記録発行装置１１５へ送るものとする。

【００５７】カード記録発行装置１１５は、新規登録許可を記録データベース１２０から受けた際、セットされているカード１４０の記録領域に暗号化装置１１４から受けた二つの暗号化データS0 , S1 を記録し、記録されたカード１４０を排出することにより発行する。

【００５８】データ通信装置１１６は、カード発行システム１１０内と記録データベース１２０との間でデータ通信網を介してデータの授受を行う通信装置である。

【００５９】記録データベース１２０は、上述されたように、カード発行システム１１０で発生した通し番号N0 および発行装置識別子M0 による特定番号と時刻データT0 と、更に利用実績初期値データV0 とを受ける。

【００６０】記録装置１２１は、通し番号N、発行装置識別子M、時刻データT、および利用実績データとして利用回数データVを記録する記憶領域を、通し番号Nおよび発行装置識別子Mによる特定番号に対応して設けるものとし、カード発行の際にはカード発行システム１１０から受けたデータを記録する。

【００６１】データ検索装置１２２は、一方ではカード発行システム１１０から発行登録のための記録要求を受けた際、該当領域にすでに記録済みの場合には新規登録不可をカード発行システム１１０へ通知する。他方、データ検索装置１２２は、図示されていないカード照合システム１３０から通し番号Nおよび発行装置識別子Mによる特定番号を受け、この特定番号に対応する領域を検索して結果をカード照合システム１３０へ送る。

【００６２】データ通信装置１２３は、カード発行システム１１０内と記録データベース１２０との間でデータ通信網を介してデータの授受を行う通信装置であると共に、カード照合の際には、図示されていないカード照合システム１３０との間のデータ授受も行う。

【００６３】次に、カード発行の際の動作手順について説明する。

【００６４】カード発行システム１１０で発生した通し番号N0 、発行装置識別子M0 、時刻データT0 、および利用実績初期値データV0 は、データ通信装置１１６，１２３を介してデータ検索装置１２２へ送られ、データ検索装置１２２は記録装置１２１で通し番号N0 および発行装置識別子M0 に対応する領域に時刻データT0 および利用回数データV0 を登録して新規登録許可をカード発行システム１１０へ返送する。この際に、既に登録済みの場合にはカード発行システム１１０へ新規登録不許可が送られる。

【００６５】カード発行システム１１０では、記録データベース１２０から新規登録許可があった際に、カード記録発行装置１１５が、カード１４０に暗号化データS3 , S4 を記録して排出することによりカード１４０を発行する。

【００６６】次に、図４を参照して第１の実施例のカード照合システム１３０について説明する。

【００６７】利用する際にカードを照合するカード照合システム１３０は、カード読取書込装置１３１、復号化

装置１３２、照合装置１３３、時刻発生装置１３４、利用実績更新装置１３５、暗号化装置１３６、およびデータ通信装置１３７を備えている。

【００６８】カード読取書込装置１３１は、利用するカード１４０をセットされた際に、カード１４０に記録されている暗号化データＳ３，Ｓ４ それぞれを読取り、復号化装置１３２へ送り、利用許可を照合装置から受けた際には暗号化装置１３６から受ける暗号化データＳ３，Ｓ５ をカード１４０に上書き記録し排出することにより、カード１４０をカード利用者に返却する。

【００６９】復号化装置１３２は、一方では、特定暗号化鍵により暗号化データＳ３ を復号して特定番号Ｎ０，Ｍ０ を生成し、データ通信装置１３７へ送り、生成された特定番号Ｎ０，Ｍ０ に基づいて記憶データベース１２０の記録装置１２１から時刻データＴ０ および利用回数データＶ０ を検索して読取り受取る。

【００７０】他方では、復号化装置１３２は、記録装置１２１から受ける時刻データＴ０ を復号化鍵として、カード読取書込装置１３１から受けた暗号化データＳ４ を復号して復号符号Ｖｄ を生成し、照合装置１３３へ送る。復号符号Ｖｄ は、正常に認証できるカード１４０であれば利用回数データＶ０ である。

【００７１】照合装置１３３は、一方で復号化手段３２から受ける復号符号Ｖｄ 、他方で記録データベース１２０から受ける利用回数データＶ０ 、両者を照合し、一致した際に利用許可をカード読取書込装置１３１へ送ると共に特定番号Ｎ０，Ｍ０ を暗号化装置１３６とデータ通信装置１３７を介して記録データベース１２０とのそれぞれへ出力するものとする。

【００７２】時刻発生装置１３４は、カード照合時刻を認識すると共に、乱数発生手段でもあり、２４時間にわたり数字を順次発生する。時刻発生装置１３４は、カード照合の際に発生する時刻データＴ１ を、暗号化鍵として暗号化装置１３５へ送ると共にデータ通信装置１３７を介して記録データベース１２０へ送り記録データを更新するものとする。

【００７３】利用実績更新装置１３５は、カード利用に際して、照合された利用回数データＶ０ を受け、１回を加算更新した利用回数データＶ１ を発生し、暗号化装置１３５へ送ると共にデータ通信装置１３７を介して記録データベース１２０へ送り記録更新するものとする。

【００７４】暗号化装置１３６は、一方で照合装置１３３から特定番号Ｎ０，Ｍ０ を受け、他方で時刻発生装置１３４が発生する時刻データＴ１ および利用実績更新装置１３５から更新された利用回数データＶ１ を受け、カード発行システム１０と同様に、一方では固定された特定暗号化鍵により特定番号Ｎ０，Ｍ０ を暗号化した暗号化データＳ３ 、他方では時刻発生装置１３４が発生した時刻データＴ１ を暗号化鍵として利用回数データＶ１ を暗号化した暗号化データＳ５ 、それぞれを生成し、カード読取書込装置１３１へ送るものとする。

【００７５】データ通信装置１３７は、カード照合システム１３０内と記録データベース１２０との間でデータ通信網を介してデータの授受を行う通信装置である。

【００７６】時刻発生装置１３４から送られる時刻データＴ１ および利用実績更新装置１３５から送られる利用回数データＶ１ は、データ通信装置１３７，１２３を介してデータ検索装置１２２へ送られ、記録装置１２１において、時刻データＴ０ および利用回数データＶ０ を上書きすることにより、時刻データＴ０ および利用回数データＶ０ それぞれの記録が時刻データＴ１ および利用回数データＶ１ それぞれに更新される。

【００７７】次に、カード照合の際の動作手順について説明する。

【００７８】カード読取書込装置１３１にカード１４０を挿入して利用する際には、カード読取書込装置１３１が挿入されたカード１４０から暗号化データＳ３，Ｓ４ を読取り、復号化装置１３２に送る。

【００７９】復号化装置１３２では、受けた暗号化データＳ３ から特定暗号化鍵により特定番号Ｎ０，Ｍ０ を再生し、この特定番号Ｎ０，Ｍ０ を記録データベース１２０へ送り、記録装置１２１の特定番号Ｎ０，Ｍ０ 対応領域から時刻データＴ０ および利用回数データＶ０ を索引する。

【００８０】次いで、復号化装置１３２が、カード読取書込装置１３１から受けた暗号化データＳ４ を記録装置１２１から索引した時刻データＴ０ を暗号鍵鍵にして復号することにより利用回数データＶｄ を再生し、利用回数データＶｄ と共に、先に記録装置１２１から索引した特定番号Ｎ０，Ｍ０ 、時刻データＴ０ 、および利用回数データＶ０ を、照合装置１３３へ送る。

【００８１】照合装置１３３は、復号化装置１３２から受けるデータ、すなわち、暗号化データＳ３ から再生したした特定番号Ｎ０，Ｍ０ により記録装置１２１から索引された利用回数データＶ０ と暗号化データＳ４ から復号した特定番号Ｎｄ とを照合する。次いで照合装置１３３は、照合一致の場合、挿入されたカード１４０の利用許可をカード読取書込装置１３１へ送ると共に、特定番号Ｎ０，Ｍ０ を暗号化手段３５へ送る。

【００８２】この利用許可にしたがってカード１４０が利用され、例えば、精算により利用が終了した際、一方では、暗号化装置１３６が、更新された時刻データＴ１ および利用回数データＶ１ を受け、この時刻データＴ１ を暗号化鍵にして利用回数データＶ１ を暗号化し、新しい暗号化データＳ５ を作成し、特定番号Ｎ０，Ｍ０ を特定暗号化鍵により暗号化した暗号化データＳ３ と共にカード読取書込装置１３１へ送る。

【００８３】また、カードの利用が終了した際、他方では、記録データベース１２０が、新しい時刻データＴ１ と利用回数データＶ１ とを受け、記録装置１２１の特定

番号N0 ，M0 領域で時刻データT1 および利用回数データV1 それぞれを上書きして更新登録する。

【００８４】また、カード読取書込手段３１は、暗号化データS3 ，S5 とを受けた暗号化データS4 に暗号化データS5 を上書きして更新記録したカード１４０を排出しカード利用者に返却することにより、カード１４０の利用を終了する。

【００８５】［第２の実施例］次に、上記実施の形態とは異なる第２の実施例について図５および図６を参照して具体的に説明する。図示されるように、電子貨幣カードの発行照合システムは複数のカード発行システム２１０、一つの記録データベース２２０、および複数のカード照合システム２３０により構成され、データ通信網を介して遠隔地間で相互接続されており、書込み読取り可能な記録媒体によるカード２４０が使用されているものとする。

【００８６】第２の実施例が第１の実施例と相違する点は、暗号化装置２２２を一つの記録データベース２２０に設け、複数のカード発行システム２１０およびカード照合システム２３０には復号化装置も備えないことである。

【００８７】まず、図５を参照して第２の実施例のカード発行システム２１０について説明する。

【００８８】カード２４０を発行するカード発行システム２１０は、特定番号発生装置２１１、時刻発生装置２１２、利用実績初期値発生装置２１３、カード記録発行装置２１４、およびデータ通信装置２１５を備えるものとする。記録データベース２２０は記録装置２２１、データ検索装置２２２、暗号化装置２２３、照合装置２２４、およびデータ通信装置２２５を備えるものとする。これら装置の基本機能は、上記第１の実施例と同一である。

【００８９】特定番号発生装置２１１は、カード発行の際に発行されるカード２４０に対して通し番号N- を順次発生し、カード１４０にシステム内で一意のカード番号を付与するため、発行装置識別子M1 を出力するものとする。通し番号N0 および発行装置識別子M1 それぞれはカード発行の際に、暗号化装置２１４およびデータ通信装置２１５それぞれへ送られる。

【００９０】時刻発生装置２１２は、現在時刻T0 を時刻データT0 として発生し、カード発行の際にデータ通信装置２１５を介して記録データベース２２０へ送る。利用実績初期値発生装置２１３は、カード２４０が未使用で利用実績がないことを示す初期値データV0 を発生して、カード発行の際にデータ通信装置２１５を介して記録データベース２２０へ送る。

【００９１】データ通信装置２１５は、カード発行システム２１０内と記録データベース２２０との間でデータ通信網を介してデータの授受を行う通信装置である。

【００９２】記録データベース２２０では、データ通信装置２２５を介して、特定番号発生装置２１１から通し番号N0 および発行装置識別子M1 、時刻発生装置２１２から時刻データT0 、更に、利用実績初期値発生装置２１３から利用実績初期値データV0 それぞれを受け、暗号化装置２２３が、時刻データT0 を暗号化鍵として利用実績初期値発生装置２１３から受ける利用実績初期値データV0 を暗号化し、この暗号化された暗号化データS6 を新規登録許可としてデータ通信装置２２５を介しカード発行システム２１０へ送る。

【００９３】カード発行システム２１０では、カード記録発行装置２１４が、新規登録許可として暗号化データS6 を記録データベース２２０から受けた際、この受けた暗号化データS6 並びに特定番号発生装置２１１から受けた通し番号N0 および発行装置識別子M1 、更に利用実績初期値発生装置２１３から受けた利用実績初期値データV0 それぞれを、セットされているカード２４０の記録領域に記録し、記録されたカード２４０を排出することにより発行する。

【００９４】一方、記録データベース２２０では、暗号化装置２２２が、カード発行システム２１０から受けた通し番号N0 、発行装置識別子M1 、時刻データT0 および利用実績初期値データV0 それぞれをデータ検索装置２２２を介して記録装置２２１へ送り、記録装置２２１において通し番号N0 および発行装置識別子M1 の特定番号に対して記録されるものとする。

【００９５】次に、図６を参照して第２の実施例のカード参照システム２３０について説明する。

【００９６】カード２４０の利用許可を認証するカード照合システム２３０は、カード読取書込装置２３１、データ通信装置２３２、時刻発生装置２３３、および利用実績更新装置２３４を備えている。また、記録データベース２２０は、図５と同様に記録装置２２１、データ検索装置２２２、暗号化装置２２３、照合装置２２４、およびデータ通信装置２２５を備えるものとする。これら装置の基本機能は、上記第１の実施例と同一名称の装置とほぼ同様である。

【００９７】従って、動作手順にしたがって説明する。

【００９８】カード読取書込装置２３１は、利用するカード２４０をセットされた際、カード２４０に記録されている通し番号N0 および発行装置識別子M1 の特定番号、暗号化データS6 、ならびに利用実績初期値データV0 それぞれを読取り、データ通信装置２３２を介して記録データベース２２０へ送る。データ通信装置２３２は、転送した通し番号N0 および発行装置識別子M1 の特定番号をカード２４０への書込みのため保持するものとする。

【００９９】記録データベース２２０では、データ通信装置２２５を介して暗号化装置２２３が通し番号N0 および発行装置識別子M1 の特定番号、暗号化データS6 、ならびに利用実績初期値V0 それぞれを、また照合

装置２２４が利用実績初期値データＶ0 を、カード照合システム２３０から受取る。

【０１００】暗号化装置２２３は、通し番号N0 および発行装置識別子M1 の特定番号に基づいてデータ検索装置２２２を介して記録装置２２１を検索し、時刻データTｏを得る。また、暗号化装置２２３は、上記カード発行の際と同様、時刻データＴ0 を暗号化鍵としてカード照合システム２３０から受ける利用実績初期値データＶ0 を暗号化し、この暗号化された暗号化データＳd 、正常であれば暗号化データＳ6 、を照合装置２２４へ送る。

【０１０１】照合装置２２４は、暗号化装置２２３から受ける暗号化データＳd と、カード照合システム２３０から受ける暗号化データＳ6 とを照合し、照合の一致により利用許可をデータ通信装置２２５を介してカード照合システム２３０へ送る。

【０１０２】また、図示されていないが、この照合装置２２４が、通し番号N0 および発行装置識別子M1 の特定番号に基づいてデータ検索装置２２２を介して記録装置２２１を検索し得た利用実績初期値データＶ0 と、カード照合システム２３０から受ける利用実績初期値データＶ0 とを照合して調べる場合、先の暗号化データと二重に照合の一致を調べることになり、照合をより一層厳しくできる。

【０１０３】カード照合システム２３０では、記録データベース２２０から受けた照合一致の信号により、時刻発生装置２３３は時刻データＴ1 、また、利用実績更新装置２３４は利用回数データＶ1 、それぞれをデータ通信装置２３２を介して記録データベース２２０へ送る。この際、データ通信装置２３２は、転送する利用回数データＶ1 を保持するものとする。

【０１０４】記録データベース２２０では、暗号化装置２２３が再び、時刻発生装置２３３から送られる時刻データＴ1 および利用実績更新装置２３４から送られる利用回数データＶ1 により、上記同様、時刻データＴ1 を暗号化鍵としてカード照合システム２３０から受ける利用回数データＶ1 を暗号化し、暗号化データＳ7 を生成する。

【０１０５】この暗号化された暗号化データＳ7 が、データ通信装置２２５，２３２を介してカード照合システム２３０へ送られる一方、暗号化装置２２３により時刻データＴ1 および利用回数データＶ1 が記録装置２２１へ送られ、上書きすることにより、時刻データＴ0 および利用回数データＶ0 それぞれの記録が時刻データＴ1 および利用回数データＶ1 それぞれに更新される。

【０１０６】他方、カード照合システム２３０では、データ通信装置２３２が暗号化データＳ7 を受け、かつカード利用の終了を知らされることにより、受けた暗号化データＳ7 と保持している通し番号N0 および発行装置識別子M1 の特定番号、並びに利用回数データＶ1 とをカード読取書込装置２３１へ送る。

【０１０７】カード読取書込装置２３１は、利用許可と利用終了とを受けた際、データ通信装置２３２から受ける暗号化データＳ7 、通し番号N0 および発行装置識別子M1 の特定番号、並びに利用回数データＶ1 をカード２４０に上書き記録し排出することにより、カード２４０をカード利用者へ返却する。

【０１０８】上記説明では、利用許可と利用終了との時期を分けて説明したが、システムの効率的な使用では、例えば精算による利用終了の際に、カードの照合によりカードの利用許可／不許可の認証が行われる。

【０１０９】また、上述したように、暗号化する対象データは上記説明に限定されない。

【０１１０】

【発明の効果】以上説明したように本発明によれば、次のような効果を得ることができる。

【０１１１】第１の効果は、改ざんのためのカード上のデータ解析が困難なことである。

【０１１２】その理由は、カード上に記録された暗号化データは、時刻データなどの乱数により、各カード、更に一つのカードでも利用の都度、異なる暗号化鍵が使用されているためである。

【０１１３】第２の効果は、カード上のデータ解析ができても偽造が困難なことである。

【０１１４】その理由は、記録データベースをカードの発行場所または照合場所と隔離し、更に、利用実績などの発行記録を暗号化データとするなどにより、偽造により暗号化データの整合性を得ることが困難なためである。

【０１１５】第３の効果は、カードの製造コストが安くあがることである。

【０１１６】その理由は、カードが単なる書込み読取り可能な安価な記録媒体でよく、カード認証のための特別な演算機能などのシステムを必要としないためである。

【図面の簡単な説明】

【図１】本発明の実施の一形態を示す機能ブロック図である。

【図２】本発明の実施の一形態を示すフローチャートである。

【図３】本発明の第１の実施例のカード発行システムを示す機能ブロック図である。

【図４】本発明の第１の実施例のカード照合システムを示す機能ブロック図である。

【図５】本発明の第２の実施例のカード発行システムを示す機能ブロック図である。

【図６】本発明の第２の実施例のカード照合システムを示す機能ブロック図である。

【符号の説明】

１０、１１０、２１０　　カード発行システム

１１　　特定番号発生手段

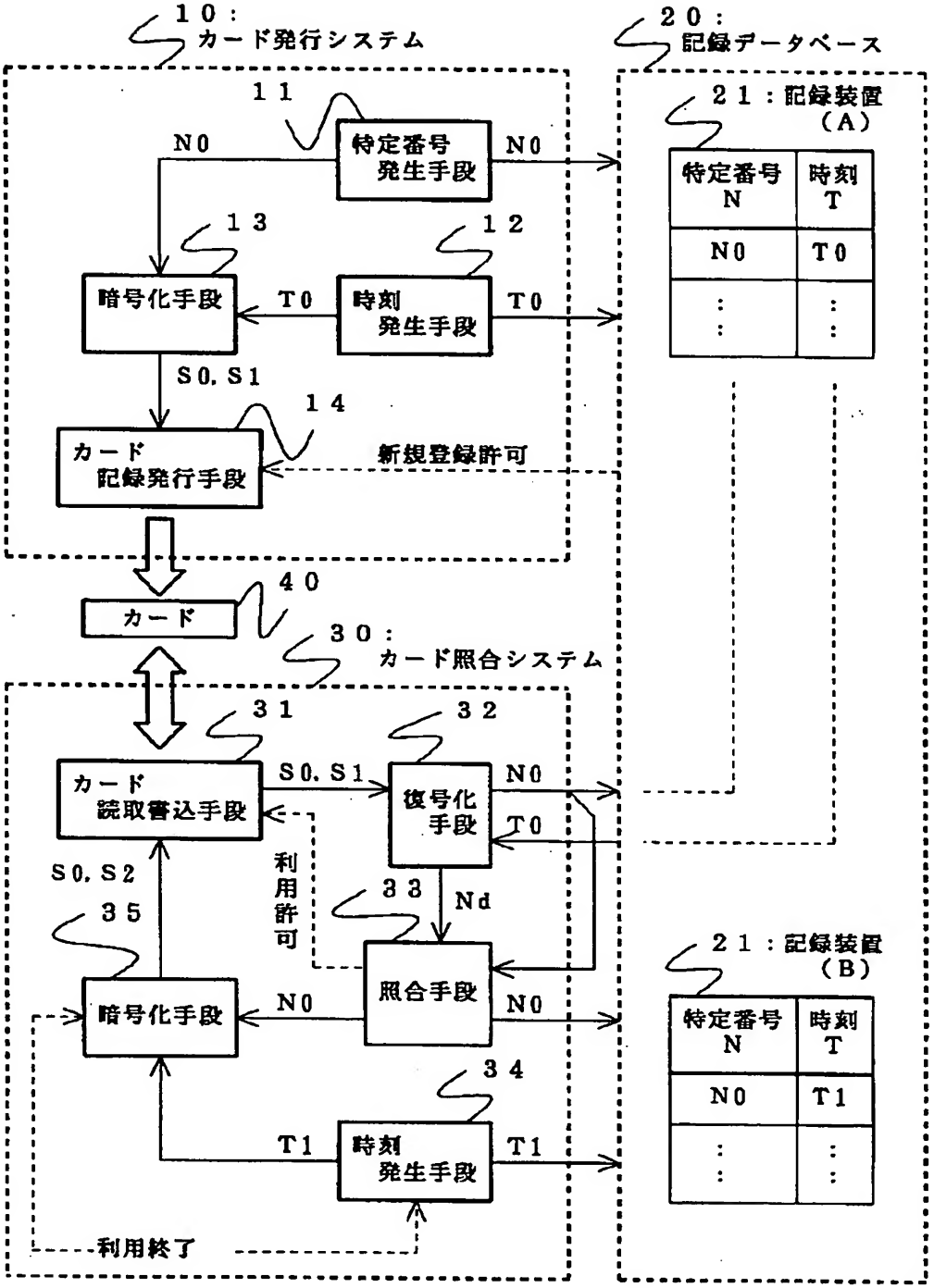
21

１２　　時刻発生手段
１３、３５　　暗号化手段
１４　　カード記録発行手段
２０、１２０、２２０　　記録データベース
２１、１２１、２２１　　記録装置
３０、１３０、２３０　　カード照合システム
３１　　カード読取書込手段
３２　　復号化手段
３３　　照合手段
３４　　時刻発生手段
４０、１４０、２４０　　カード
１１１、２１１　　特定番号発生装置

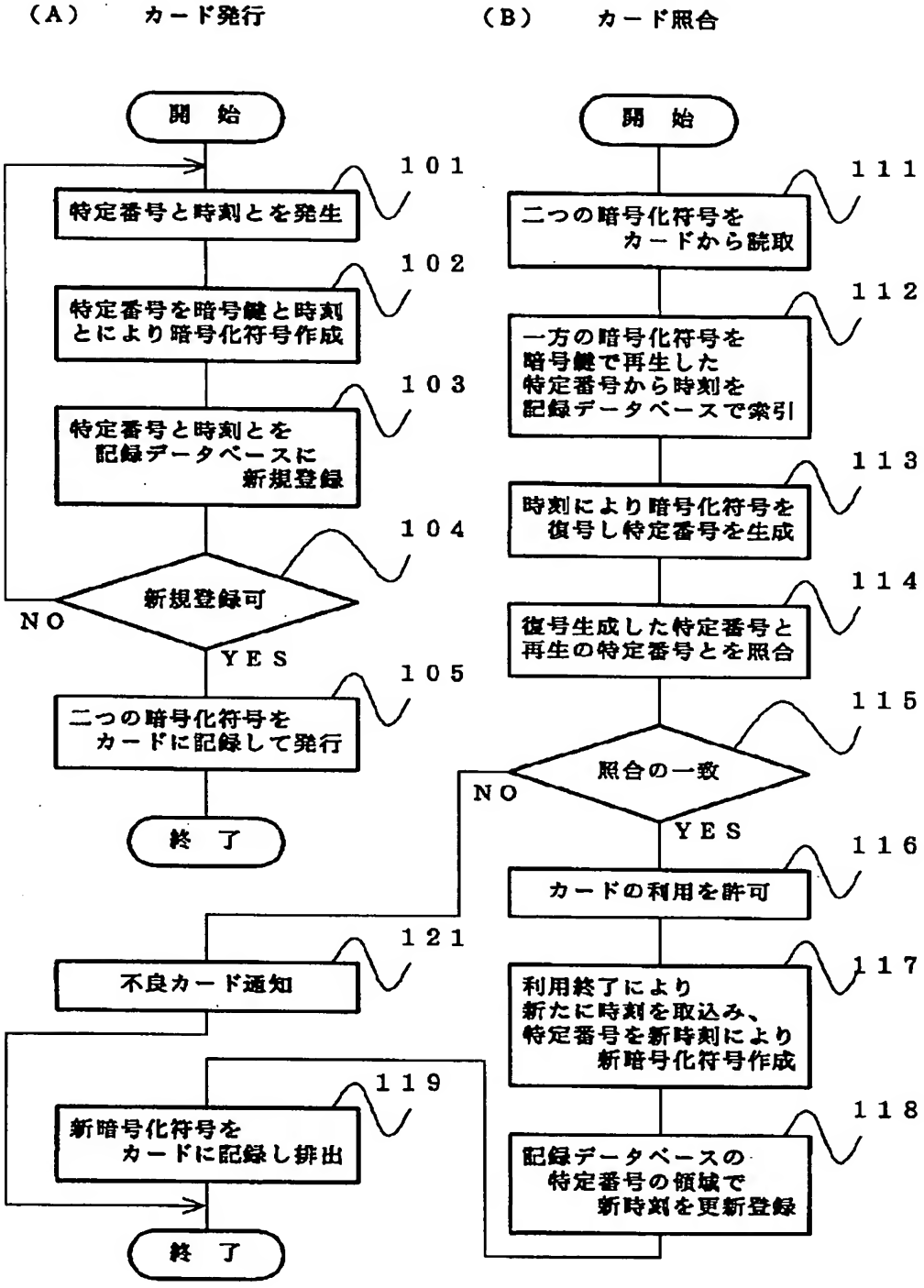
22

１１２、１３４、２１２、２３３　　時刻発生装置
１１３、２１３　　利用実績初期値発生装置
１１４、１３６、２２３　　暗号化装置
１１５、２１４　　カード記録発行装置
１１６、１２３、１３７、２１５、２２５、２３２　　データ通信装置
１２２、２２２　　データ検索装置
１３１、２３１　　カード読取書込装置
１３２　　復号化装置
１３３、２２４　　照合装置
１３５、２３４　　利用実績更新装置

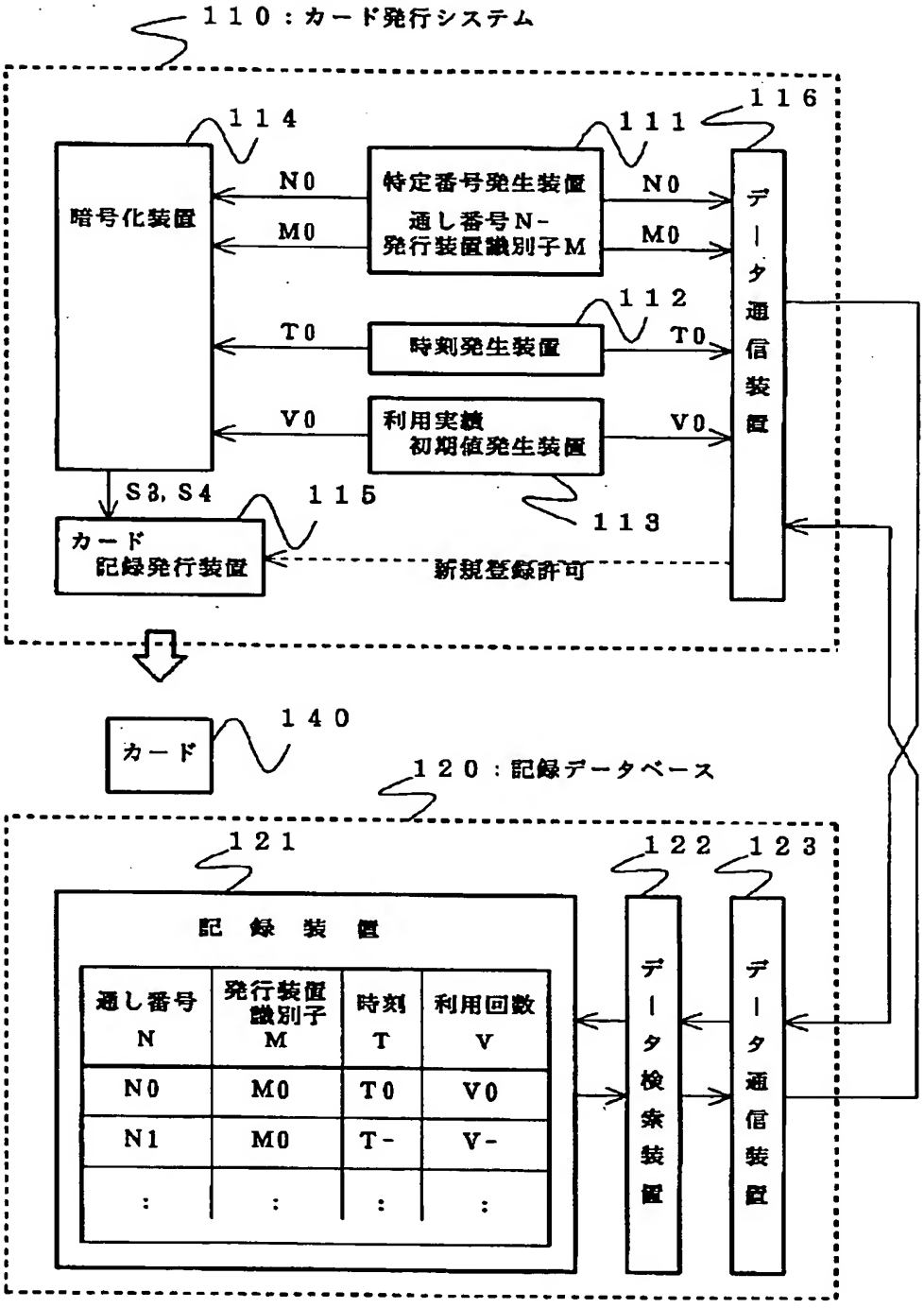
【図１】


１０：
カード発行システム
２０：
記録データベース
１１
特定番号
発生手段
N0
N0
２１：記録装置
（A）
特定番号
N
時刻
T
N0
T0
１３
１２
暗号化手段
T0
時刻
発生手段
T0
S0, S1
１４
カード
記録発行手段
新規登録許可
４０
カード
３０：
カード照合システム
３１
３２
カード
読取書込手段
S0, S1
復号化
手段
N0
T0
S0, S2
利用許可
３３
Nd
３５
２１：記録装置
（B）
暗号化手段
N0
照合手段
N0
特定番号
N
時刻
T
N0
T1
３４
T1
時刻
発生手段
T1
利用終了

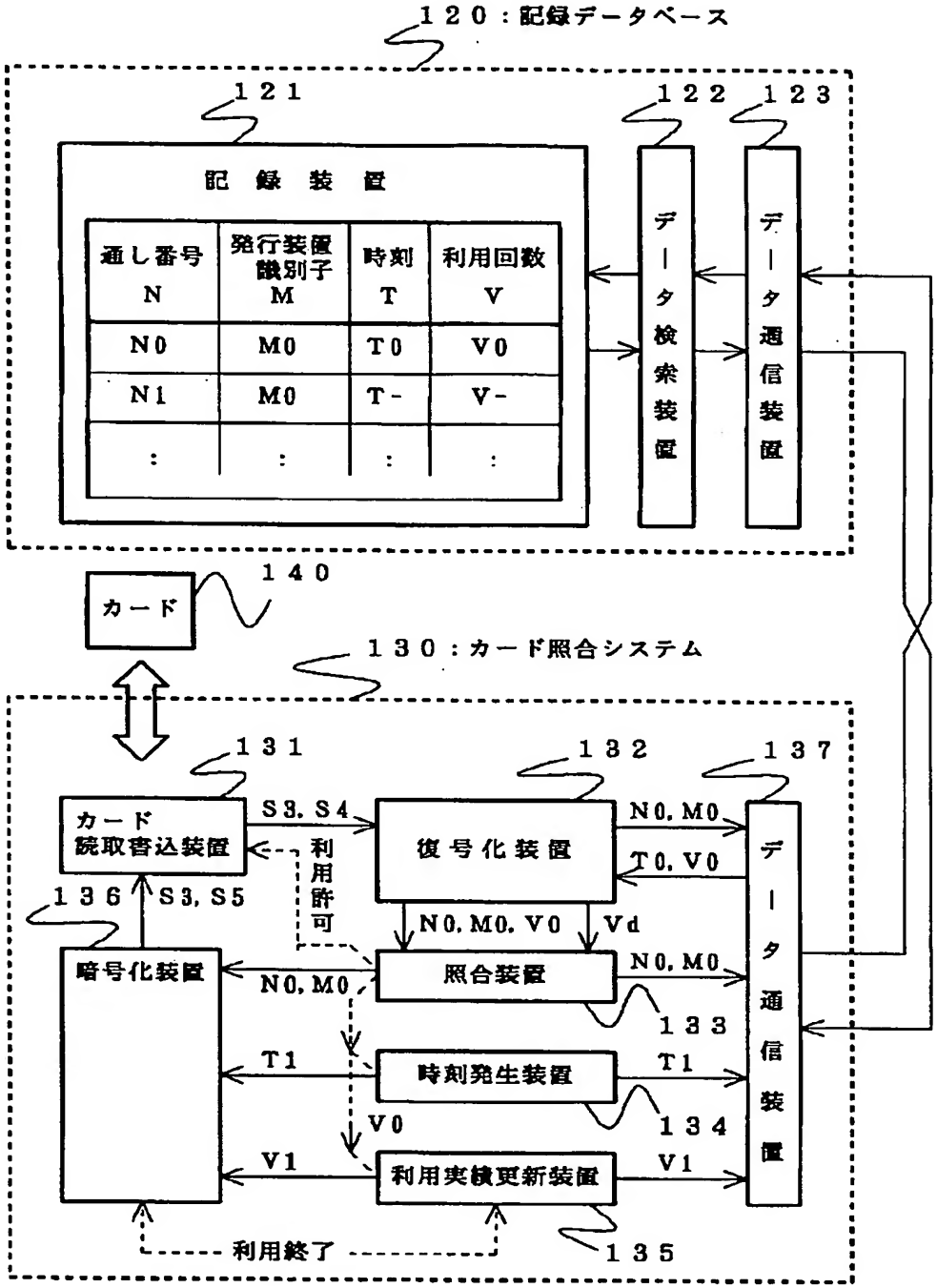
【図２】


（A）　カード発行
開　始
101
特定番号と時刻とを発生
102
特定番号を暗号鍵と時刻とにより暗号化符号作成
103
特定番号と時刻とを記録データベースに新規登録
104
新規登録可
NO
YES
105
二つの暗号化符号をカードに記録して発行
終　了
（B）　カード照合
開　始
111
二つの暗号化符号をカードから読取
112
一方の暗号化符号を暗号鍵で再生した特定番号から時刻を記録データベースで索引
113
時刻により暗号化符号を復号し特定番号を生成
114
復号生成した特定番号と再生の特定番号とを照合
115
照合の一致
NO
YES
116
カードの利用を許可
117
利用終了により新たに時刻を取込み、特定番号を新時刻により新暗号化符号作成
118
記録データベースの特定番号の領域で新時刻を更新登録
121
不良カード通知
119
新暗号化符号をカードに記録し排出
終　了

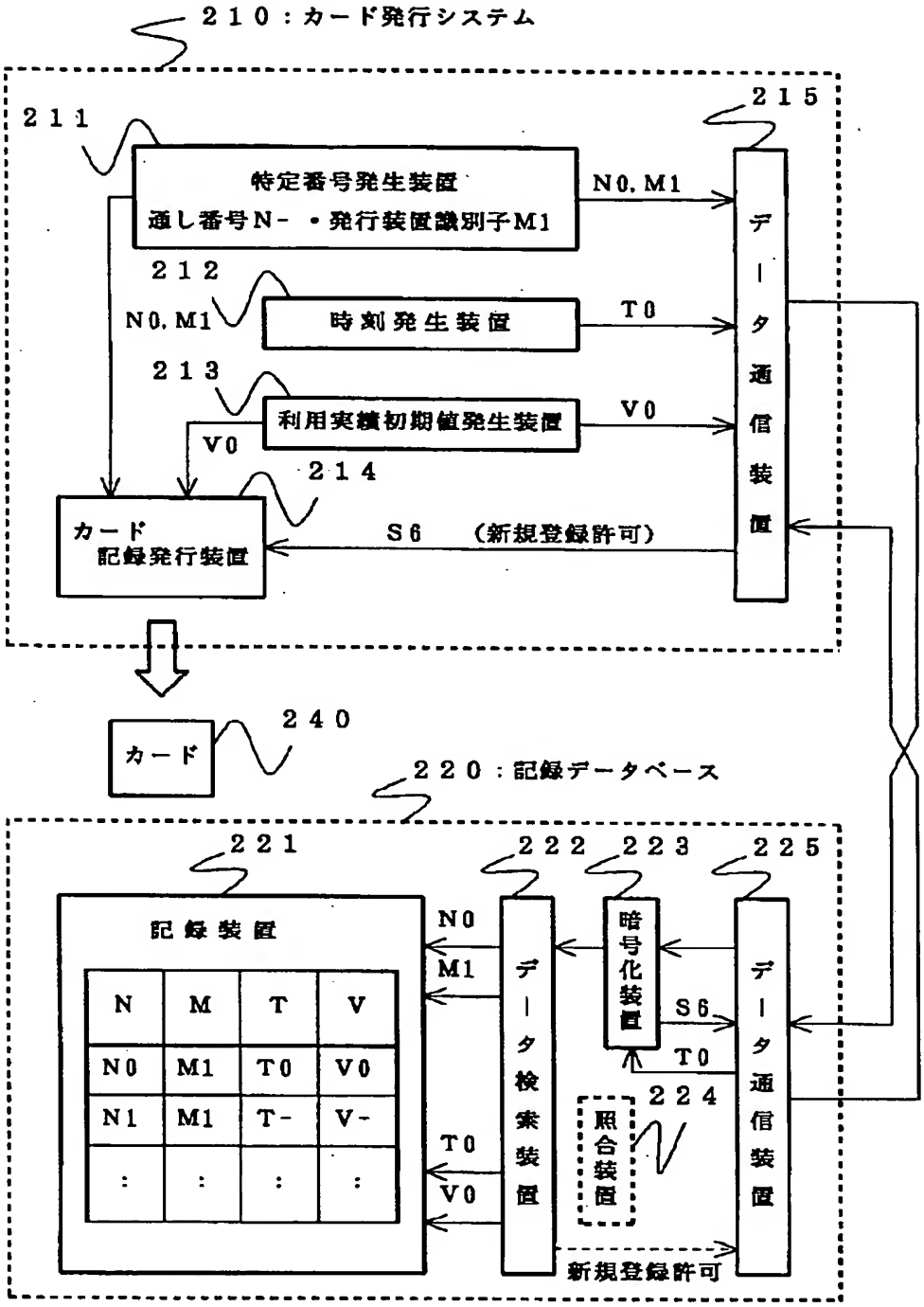
【図３】


１１０：カード発行システム
１１４
１１１
１１６
暗号化装置
特定番号発生装置
通し番号Ｎ－
発行装置識別子Ｍ
データ通信装置
Ｎ０
Ｍ０
Ｔ０
Ｖ０
１１２
時刻発生装置
利用実績
初期値発生装置
Ｓ３，Ｓ４
１１５
１１３
カード
記録発行装置
新規登録許可
カード
１４０
１２０：記録データベース
１２１
１２２
１２３
記　録　装　置
通し番号
Ｎ
発行装置
識別子
Ｍ
時刻
Ｔ
利用回数
Ｖ
Ｎ０
Ｍ０
Ｔ０
Ｖ０
Ｎ１
Ｍ０
Ｔ－
Ｖ－
：
：
：
：
データ検索装置
データ通信装置

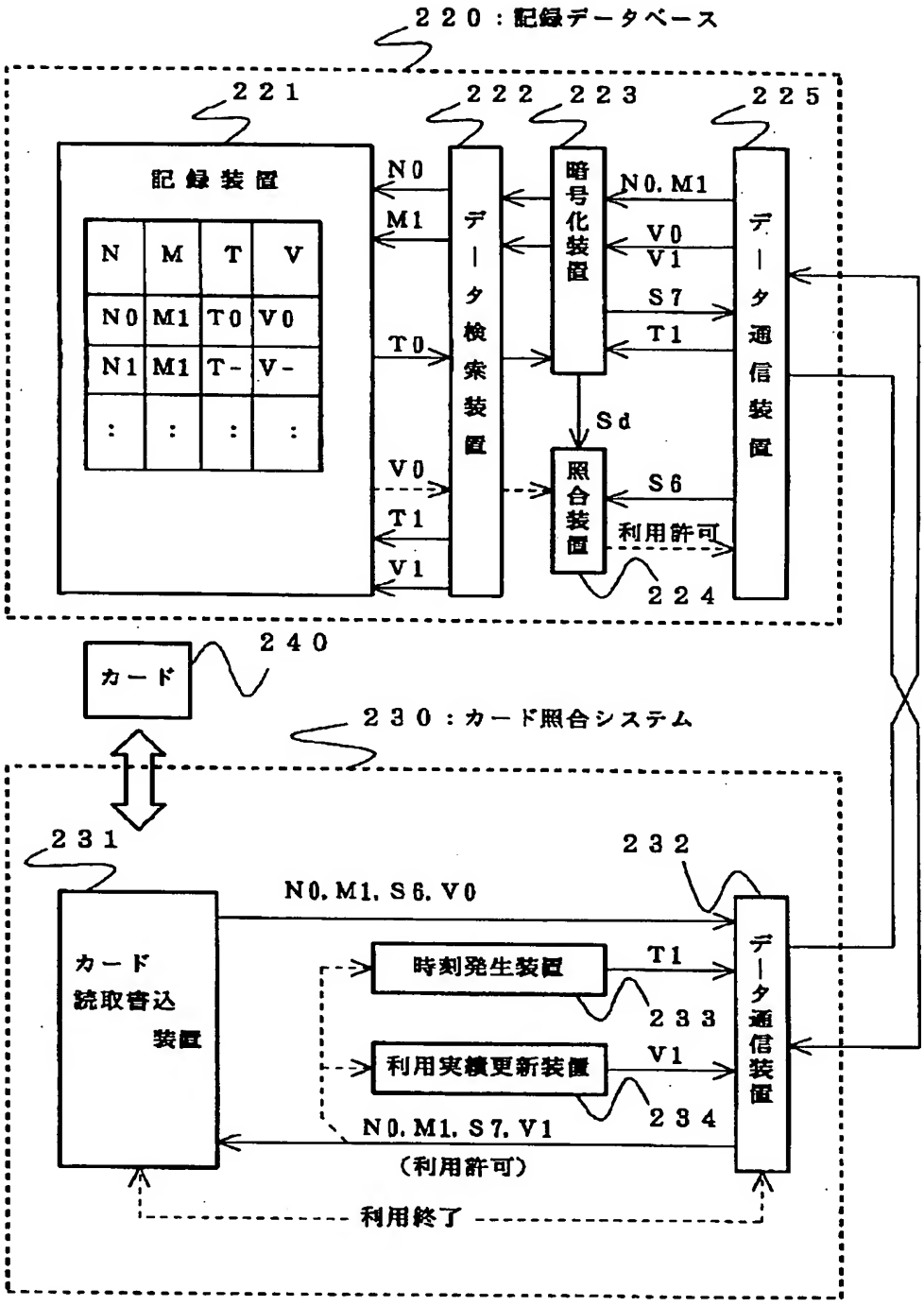
【図４】


１２０：記録データベース
１２１
１２２
１２３
記　録　装　置
通し番号 N
発行装置識別子 M
時刻 T
利用回数 V
N0
M0
T0
V0
N1
M0
T-
V-
データ検索装置
データ通信装置
１４０
カード
１３０：カード照合システム
１３１
１３２
１３７
カード読取書込装置
S3, S4
利用許可
復号化装置
N0, M0
T0, V0
１３６
S3, S5
N0, M0, V0
Vd
暗号化装置
照合装置
N0, M0
１３３
T1
時刻発生装置
T1
１３４
V0
V1
利用実績更新装置
V1
利用終了
１３５
データ通信装置

【図５】


２１０：カード発行システム
２１１
特定番号発生装置
通し番号N－・発行装置識別子M1
N0, M1
２１５
データ通信装置
２１２
N0, M1
時刻発生装置
T0
２１３
利用実績初期値発生装置
V0
V0
２１４
カード記録発行装置
S6　（新規登録許可）
２４０
カード
２２０：記録データベース
２２１
記録装置
N　M　T　V
N0　M1　T0　V0
N1　M1　T－　V－
：　：　：　：
２２２
データ検索装置
２２３
暗号化装置
２２５
データ通信装置
N0
M1
T0
V0
S6
T0
２２４
照合装置
新規登録許可

【図６】



フロントページの続き

(51)Int.Cl.⁶	識別記号	FI	
G07F 7/08		G06F 15/30	340
G07G 1/12	321		350A
		G07F 7/08	M